Case Study: Application Versus Network Redundancy

Dorran Bekker
Consolidated Power Projects Ltd.

Timothy Tibbals, Normann Fischer, and Chris Ewing
Schweitzer Engineering Laboratories, Inc.

Presented at the
3rd Annual Protection, Automation and Control World Conference
Budapest, Hungary
June 25–28, 2012

Originally presented at the
14th Annual Western Power Delivery Automation Conference, March 2012

Case Study: Application Versus Network Redundancy

Dorran Bekker, *Consolidated Power Projects Ltd.*
Timothy Tibbals, Normann Fischer, and Chris Ewing, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—The use of digital communications, including IEC 61850 Generic Object-Oriented Substation Event (GOOSE), for protection and control purposes has created opportunities to eliminate hard-wired copper terminations to exchange data and status values among intelligent electronic devices (IEDs). The use of digital communications (in particular, Ethernet communication) for these purposes requires that the connections and networking be robust and secure enough for the intended applications. The requirements of the application and the requirements of the communications network are often specified and evaluated separately. A result of this separation of requirements is that the network redundancy methods are applied independent of the applications that use the network.**

The independent application of network redundancy creates communications network designs that are not optimized to achieve the requirements of the applications. Often, the resulting networks are more complex than necessary. This paper discusses a best engineering practice of designing the Ethernet communications network based on the application requirements without directly specifying an Ethernet network redundancy method. In essence, it is a bottom-up approach to Ethernet network design based on protection and control requirements.

I. Introduction

Electrical substation instrumentation and control systems use a variety of topologies, networks, and protocols to communicate between multiple nodes. Typical nodes include the following:

- Intelligent electronic devices (IEDs), such as protective relays, meters, and dedicated controllers.
- Local computers, programmable logic controllers, or programmable automation controllers, providing data concentration and automatic control.
- Local displays or human-machine interfaces (HMIs).
- Wide-area network (WAN) links, including the following:
  - Supervisory control and data acquisition (SCADA) masters located in control centers.
  - Wide-area measurement and control (synchrophasor) systems.
  - Remote engineering access and maintenance workstations.
  - Event report gathering and analysis systems.

Switched Ethernet has emerged as the communications network of choice; however, network topologies vary widely with no established industry practice [1]. This paper focuses on the communications and network topologies necessary to support protection and control applications. The use and application of these communications networks vary between the substations and applications of transmission systems and those of distribution systems.

II. Historical Application Redundancy

A. Present Day Dual Main Protection Schemes

In any power system, there exists a nonzero probability that a protection scheme is out of service or unavailable at the instant a fault occurs in the protected zone. In subtransmission or distribution networks, it is often considered acceptable to have the fault cleared by the less expensive, less functional, and perhaps slower-acting local or remote backup protection, in the event of the local main protection scheme not being available. In transmission networks, it is unacceptable to have faults cleared by local or remote backup protection because a delay can result in a large network disturbance and can even threaten the stability of the power system. To reduce the probability of a main transmission protection scheme being unavailable during a fault condition, transmission protection schemes are composed of a dual main protection scheme—two independent and fully functional protection schemes. A dual main protection scheme typically comprises a Main 1 and Main 2 protection system. These two systems may be duplicates of one another; however, they share no commonality with one another, which acts to reduce the possibility of a common-mode failure. The only thing that these two systems have in common with one another is that they operate the same circuit breaker. Fig. 1 is a sketch showing a traditional dual main protection scheme.

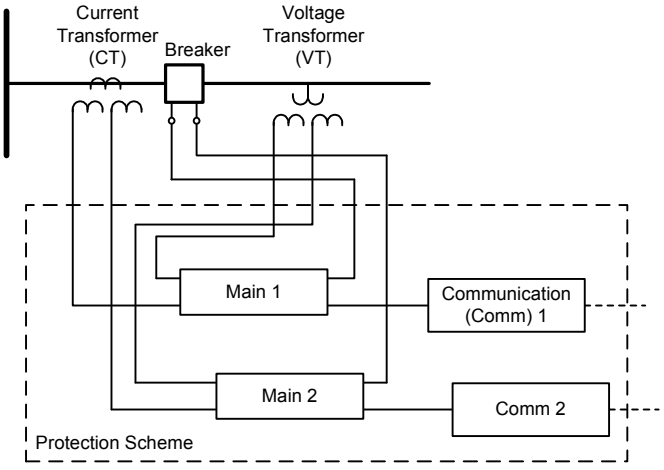

Fig. 1. Simple sketch of a dual main protection system that is typical of a transmission protection scheme.

B. Independent Protection Systems

From Fig. 1, we see that the two systems are autonomous from one another and they operate (function) totally independent from one another. This means that Main 1 makes decisions without input from Main 2 and vice versa. If the protected zone experiences a fault, both systems operate in parallel and independent of one another. Whichever system reaches a tripping decision first is the one to trip the circuit breaker. A protection scheme like this has many advantages in that the protection systems are completely independent and should one system fail, the integrity of the protection scheme and that of the protected zone are not compromised. Any single or multiple failures of any components in one of the protection systems or the failure of an entire individual system does not compromise the scheme.

Let us assume a transmission protection scheme is composed of dual distance relays and that one of these protection systems experiences a single component failure, as illustrated in Fig. 2.

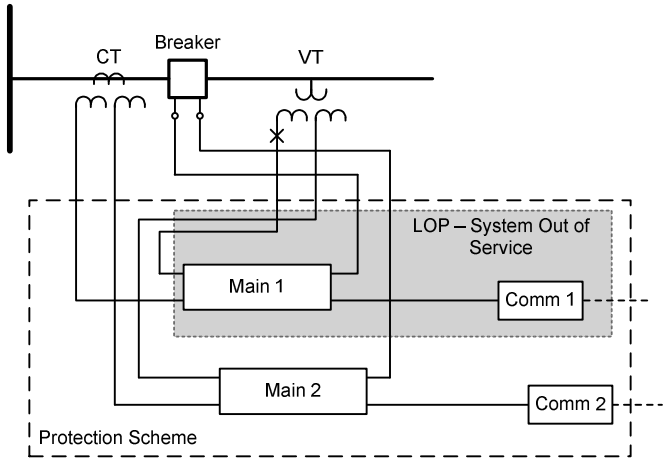

Fig. 2. Protection scheme integrity being maintained even though one main is out of service.

The Main 1 system in Fig. 2 experiences a loss-of-potential (LOP) condition, thus making the Main 1 distance elements inoperative and reducing the protection afforded by Main 1. Note that Main 1 does not become completely inoperable; it still provides backup protection via its 50/51 elements.

However, Main 2 remains fully functional and thus provides complete protection scheme functionality for the protected zone. When Main 1 experiences an LOP condition, the Main 1 protection scheme asserts an alarm condition, indicating that the system is experiencing an LOP condition and that Main 1 is not fully functional. This alarm condition is then used to notify maintenance personnel of this situation.

Many utilities further reduce the possibility of any common-mode failure through the application of protective relays with different operating principles. For example, Main 1 protection may use a distance relay for protection, whereas Main 2 may use a differential relay for protection. The merits of this are not discussed in this paper, but the general consensus among protection engineers is that a perceived weakness in one principle is covered by a strength in the other, thereby the two operating principles complement one another.

C. Simplified Protection System Testing

A further advantage of the dual main protection scheme is the ability to take one protection system out of service for maintenance or testing without compromising the integrity of the scheme. If, for instance, there is an issue with one of the main protection systems, that system can easily be taken out of service and tested without compromising the integrity of the protection scheme. Fig. 3 shows the Main 2 protection system being tested during routine maintenance or troubleshooting. Because the two systems are autonomous, no special consideration or precautions have to be taken while testing the Main 2 protection system. This makes maintenance easier and lowers the chance of a misoperation of the protection scheme while one system is undergoing maintenance or troubleshooting.

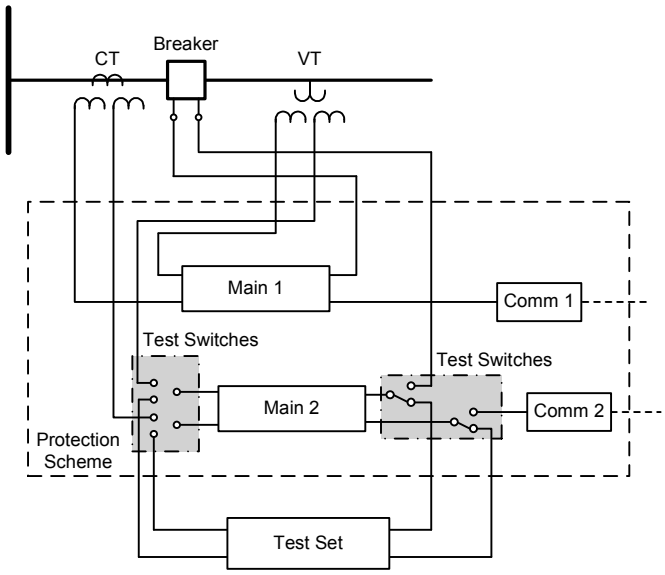

Fig. 3. Protection main being taken out of service for testing or troubleshooting without compromising the integrity of the protection scheme.

As can be seen from Fig. 3, the use of dual autonomous protection schemes with built-in test switches makes it easy for test personnel to isolate protection systems and test and troubleshoot a main protection system without unnecessarily compromising the integrity of the protection scheme or the protected system. It is for this reason that these schemes have found favor in many transmission protection systems.

Some network designers go so far as to include triple modular redundant main protection so that when any one system is removed from service, dual main protection remains. Others install two pairs of dual main protection with forethought for future obsolescence and replacement. With this method, while one dual main system is being physically replaced during an upgrade, the second dual main system remains in service.

III. Historical Network Redundancy

Data communications networks from all industries typically require redundancy at some level. Corporate communications systems are created with failover mechanisms to keep critical servers online in the event of a network failure, such as an Ethernet switch or router failure. Failover requirements for these types of applications are typically on the order of seconds and, for the most part, are transparent to the end users of these systems. These corporate-level systems are designed for the asynchronous exchange of files and email and business intelligence system access, which do not require deterministic message delivery and are therefore not impacted by a network failure event.

Communications networks are typically designed to withstand communications device failures by utilizing ring and mesh topologies (Fig. 4) and interconnecting switches to provide redundancy at the network level. These practices do not affect the performance of the end devices performing the protection and automation applications as part of the schemes. Protocols, such as Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol, were designed to support these communications topologies and provide loop-free redundant paths to end devices. Without these protocols, network loops would be present on the network and communications would be impacted by Ethernet frames circulating endlessly throughout the network. STP ensures a loop-free network and provides an alternate path to take in the event of a network failure.

In contrast to corporate communications needs, electric power system communications are typically device-to-device communications, with the occasional user interacting for engineering access to perform maintenance. These device-to-device communications are mission critical, and a network failure causing a missing or delayed packet in a protection scheme at precisely the wrong time can turn a power system malfunction into a catastrophe.

Communications systems are often specified and designed independent of connected devices and do not account for the applications the communications need to support. This becomes more prevalent as communications designers are relied upon to engineer the sophisticated and complex network devices and settings required. Redundant network communications using failover may be appropriate for applications such as SCADA, engineering access, and automation. This same network design, however, does not meet the requirements of applications requiring more deterministic network behavior or a network designed to support protection application redundancy. Though skilled in the art of communications technology, these communications design experts rarely understand the fundamentals of the protection and automation functions within the protection schemes. Worse is that communications designers often mistake communications redundancy for application redundancy and do not recognize the ramifications of message latency in mission-critical systems. Most communications network designers perceive that networks need to satisfy asynchronous SCADA systems, so even if they witness message delays and dropped packets, they are not trained to recognize these as unacceptable for peer-to-peer mission-critical applications. Networks must be designed to accommodate the true required performance of the application they support and nothing less.

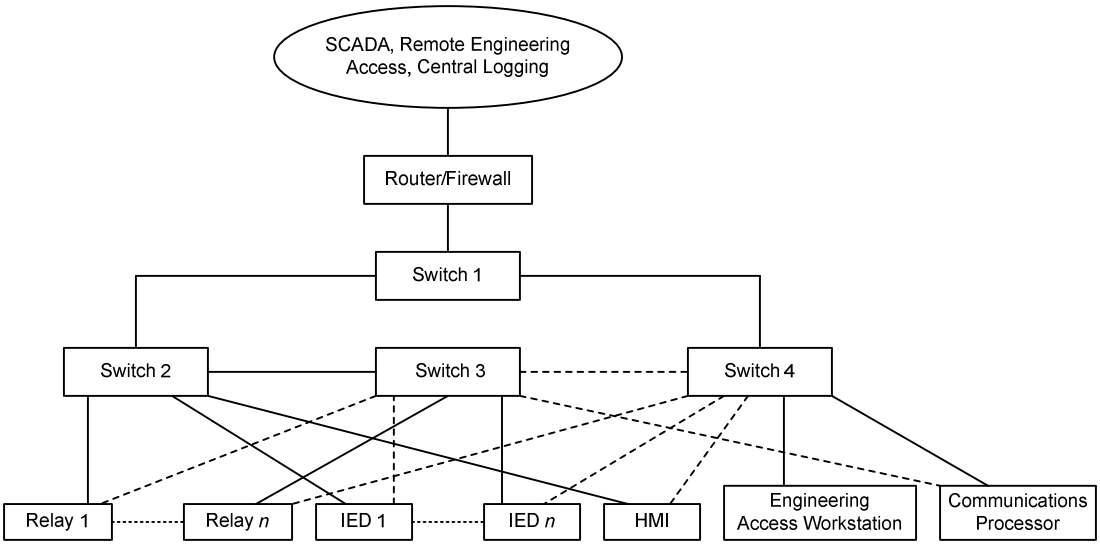

Fig. 4. Combined ring and mesh network topology example.

IV. Network Design to Support Application Redundancy

In critical applications, one of the standard redundant configurations is to have a Main 1 and Main 2 or backup protection system. This is only truly redundant when the complete systems function independent of each other. An example of such a system is used in the transmission substations of the Namibian power utility, NamPower [2]. From the beginning of the design, the different systems were independent of each other, with dedicated CT cores, dual HMIs, dual gateways, and dual dc systems. This substation design also makes use of Ethernet networks and the communications technologies that they bring, such as IEC 61850, engineering access services, and constant remote monitoring of system performance.

In these NamPower substations, the station I/O and status points are wired to I/O units capable of IEC 61850 communications. These data are then communicated to substation IEDs requiring these I/O via IEC 61850 Generic Object-Oriented Substation Event (GOOSE) messages. The use of GOOSE messages reduces the amount of substation wiring for I/O, while maintaining a maximum level of redundancy. The dual HMI and gateway systems are designed, like the protection systems, to be totally redundant and independent.

NamPower chose to use GOOSE messaging for its application to replace physical wiring with digital communications. This reduction in wiring is particularly obvious when dealing with bus zone applications. Another advantage GOOSE digital communication brings is the ability to have the status and trip signals sent via the redundant networks. Digital messaging enables the system to monitor the communications status of messages being sent or received. This monitoring allows the system to alert when a communications issue is detected rather than having an operation fail and only knowing of the failure after the fact.

Because vital protection and control information is now transmitted and received across the substation network, the protection and control IEDs are not the only redundancy requirement. The substation network now has the same considerations as the protection system, Main 1 and Main 2, similar to the networks shown in Fig. 5. The NamPower design included the network for a total Main 1 and Main 2 system, both receiving the same dual dc power supplies as the IEDs.

A further redundancy path was added, connecting the backbones of both networks together. This was to allow communications to continue in the event of a failure on two different IEDs on two different network points.

While redundancy provides protection against failures, it cannot repair a broken connection. Thus, if broken connections or functions are not monitored and reported when faulty, all the redundancy does is delay a failure. NamPower makes use of IED self-monitoring, along with Ethernet diagnostics via Simple Network Management Protocol communication to the network devices to monitor IED and network connections and devices. All collected data are sent through the gateway to the national control center so that when a failure occurs, operators and maintenance staff are informed and can diagnose most problems remotely and dispatch the appropriate personnel with necessary equipment.

Engineering access services like these are important but are still secondary to the protection system. Remotely accessing logs or events can require the transfer of large files. This network traffic must not impact the protection and control system. In the NamPower design, extensive use of virtual local-area networks separates the different services, such as engineering access, Voice over Internet Protocol, security cameras, and, most importantly, GOOSE messaging.

To make sure none of the engineering access services interfere with the protection or SCADA functions, a dedicated engineering workstation is used. This workstation is used to monitor the network and store all configurations locally. Access to this workstation via the corporate network allows personnel to access configurations and performance reports remotely.

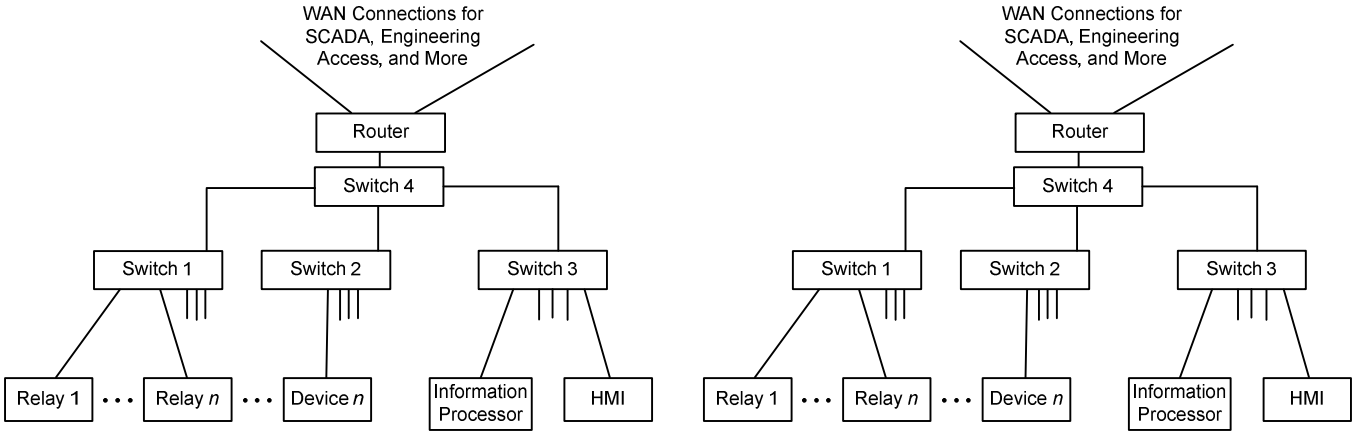

Fig. 5. Fully independent dual networks with redundant devices.

V. System Design to Support Reliability Requirements

Today, the information that SCADA systems exchange with control centers is considered mission critical, providing situational awareness to system dispatchers and real-time information for fast-acting real-time control systems. Modern SCADA system specifications often require 99.999 percent availability.

Protective relays monitor inputs to detect faults on power lines and apparatus and perform automatic high-speed control actions to disconnect power from faults.

High-voltage equipment control, such as communications-based tripping, is accomplished by using IEC 61850 GOOSE messages [3]. Delays in message delivery can lead to protection system misoperation, failure to trip, or inadequate coordination. Redundant systems are mandatory [4].

Protection and automatic control systems often require availability of at least 99.999 percent.

VI. Reliability of System Designs

The most reliable configuration is a primary network for the primary devices and a fully independent dual primary network connected to a full set of dual primary devices [5]. Virtually all extra-high-voltage and only some high-voltage transmission substations have fully redundant backup protection and monitoring devices. For other stations, cost tradeoff considerations lead to the evaluation of networks without redundant monitoring and protection devices but that do use redundancy at the network level, as shown in Fig. 6.

To calculate the availability for each topology, we used the mean time between failures (MTBF) and calculated the availability shown in Table I from data in [6]. To analyze systems with specific components, use the MTBF from the component manufacturer and the methods described in [5] and [6].

The comparison calculations are based on 22 local station relays. For the case where the application is redundant, two sets of 22 relays were used in the calculations. Table II summarizes the unavailability of the Ethernet network topologies. The unavailability numbers are normalized as numbers multiplied by 10^{-6}. In other words, unavailability is shown in units of ppm of time. To aid in visualization, an unavailability of 504 ppm is 265 minutes in a year. This is, however, the statistical average. In reality, we would expect that one of ten systems in a year would experience one 2-day outage. This is the equivalent of a network MTBF of 10.9 years, where failure is defined as the inability of the network to perform the required tasks with a mean time to repair of 2 days.

TABLE I
COMPONENT RELIABILITY DATA

Component	MTBF (years)	Unavailability (Parts Per Million [ppm])	Availability (%)
Monitored Ethernet cable	5,000	1.1	99.9999
Relay or control IED	200	27	99.9973
Ethernet switch or router	60	96	99.99040

TABLE II
SYSTEM RELIABILITY COMPARISONS

Topology	Unavailability (ppm)	
	Network Only	Network and Relays
Single network	504	1,107
Single network with redundant paths	217	820
Dual networks with failover	0.3	603
Dual redundant path networks with failover	0.1	603
Independent dual networks with redundant devices	0.3	1.2

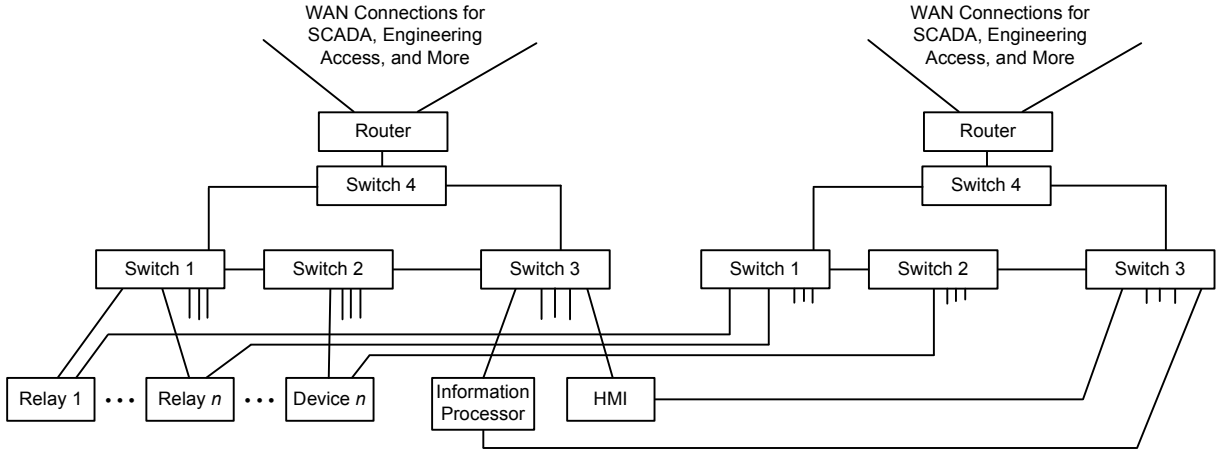

Fig. 6. Dual redundant path networks with failover.

In evaluating the impact of reliability, based on the results of the fault tree calculations shown in Table II, it is clear that redundancy does matter. However, to achieve redundancy from the application perspective, it is necessary to look at the combined nature of the system. The "Network and Relays" column in Table II represents the view of the application. In modern substations, the protection and control system relies on the network, which replaces the hard-wired I/O connections with digital communications. As a result, to truly make this system redundant, it requires independent dual networks with redundant devices. Without these completely dual systems, improvements are seen for the subcomponents where redundancy is applied but the full requirement for the application to be redundant is not achieved.

It should also be noted that new redundancy standards, such as Parallel Redundancy Protocol and High-Availability Seamless Ring, address only network redundancy from a single-IED perspective. They give network designers a false sense of security in designing resilient networks to support true application, or protection scheme, redundancy. Expanding these concepts to the application redundancy addressed in this paper doubles the networking needed to support these protocols.

VII. Conclusion

In this paper, we identify the weaknesses in redundant failover schemes that are not focused on application redundancy but rather network redundancy alone. Keeping requirements for network and protection systems independent limits the effectiveness of the end system. Engineers must apply existing technologies and equipment to implement completely redundant systems that include the Ethernet networks to meet the requirements of the application.

Demonstration of the contrast of several topologies using available equipment shows the importance of understanding the fundamentals of the protection scheme application and its redundancy, not just redundant paths for digital messages. The provided engineering analysis tools weigh the tradeoffs for specific alternatives and applications. Existing equipment can be successfully deployed in networks using switching failover methods for SCADA and other relatively low-speed applications. However, for real-time breaker control or high-speed, wide-area control systems, the failover recovery times do not typically meet the required operation times. Ethernet networking for these high-speed applications requires fully redundant systems that do not rely on failover to provide either the required performance or the required reliability.

VIII. References

[1] G. W. Scheer and D. J. Dolezilek, "Comparing the Reliability of Ethernet Network Topologies in Substation Control and Monitoring Networks," proceedings of the 2nd Annual Western Power Delivery Automation Conference, Spokane, WA, April 2000.

[2] D. D. Bekker, P. Diamandis, and T. Tibbals, "IEC 61850 – More Than Just GOOSE: A Case Study of Modernizing Substations in Namibia," proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.

[3] IEC 62271-3, *High-Voltage Switchgear and Controlgear – Part 3: Digital Interfaces Based on IEC 61850*, June 2006.

[4] L. Andersson, K. Brand, C. Brunner, and W. Wimmer, "Reliability Investigations for SA Communication Architectures Based on IEC 61850," proceedings of the IEEE Russia PowerTech Conference, St. Petersburg, Russia, June 2005.

[5] P. M. Anderson, *Power System Protection*, New York: The Institute of Electrical and Electronics Engineers, Inc., 1999.

[6] D. Costello, "Fly Safe and Level: Customer Examples in Implementing Dual Primary Protection Systems," June 2007. Available: http://www.selinc.com.

IX. Biographies

Dorran Bekker received his BSCE in 2007. After working at e-LEK Engineering as an application engineer for a year, he joined Consolidated Power Projects as a SCADA/automation engineer.

Timothy Tibbals received his BSEE from Gonzaga University in 1989. After graduation, he joined Schweitzer Engineering Laboratories, Inc. (SEL) as an application engineer, performing system studies and relay testing. Tim has also worked as a development engineer and as part of the development team for many of the communications features and functions of SEL products. He subsequently worked as an application engineer for protection, integration, and automation products, assisting customers through product training, seminars, and phone support. Tim served as the automation services supervisor in the SEL systems and services division for several years before returning to the research and development division as a product engineer for automation and communications engineering products. He is currently a senior automation system engineer in the sales and customer service division.

Normann Fischer received a Higher Diploma in Technology, with honors, from Witwatersrand Technikon, Johannesburg in 1988, a BSEE, with honors, from the University of Cape Town in 1993, and an MSEE from the University of Idaho in 2005. He joined Eskom as a protection technician in 1984 and was a senior design engineer in the Eskom protection design department for three years. Normann then joined IST Energy as a senior design engineer in 1996. In 1999, he joined Schweitzer Engineering Laboratories, Inc. as a power engineer in the research and development division. Normann is a member of IEEE and ASEE.

Chris Ewing is a lead product engineer with the Schweitzer Engineering Laboratories, Inc. (SEL) security solutions division. Prior to joining SEL, he consulted as an information security engineer in both the private and public sectors. Chris received his BS in computer science and his MS in network security, and he holds the CISSP professional security certification. He has over ten years of experience in the cybersecurity field.